

Siegel modular forms mod p

R.Weissauer

Let R be a commutative ring with unit. Assume $1/2 \in R$. For a prime p let \mathbb{F}_p denote the prime field of characteristic p and $\overline{\mathbb{F}}_p$ an algebraic closure. We always assume $p \neq 2$.

The moduli stack $A_{g,R}$. Let $g \geq 2$ be an integer. Consider the moduli stack $A_{g,R}$ of isomorphism classes of the following data (S, A, λ)

a ring homomorphism $R \rightarrow S$ of commutative rings,

an abelian scheme $A \rightarrow \operatorname{Spec}(S)$ of relative dimension g together with its zero section $e : \operatorname{Spec}(S) \rightarrow A$,

a principal polarization $\lambda : A \rightarrow A^\vee$ over $\operatorname{Spec}(S)$.

To (S, A, λ) we associate the sheaf of invariant relative differential forms $\Omega_A = e^*(\Omega_{A/S}^1)$, which is a projective rank 1 module $\omega = \Lambda^g(\Omega_A)$ on S functorial with respect to base change.

Modular forms. By definition a modular form of integral weight k and genus g over R is an assignment

$$(S, A, \lambda) \mapsto f(S, A, \lambda) \in \Gamma(\operatorname{Spec}(S), \omega^{\otimes k})$$

with the following functorial properties

- (i) Basechange compatibility: For ring homomorphisms of commutative rings $S \rightarrow S'$ one has

$$f(S', A \times_{\operatorname{Spec}(S)} \operatorname{Spec}(S'), \lambda \times_{\operatorname{Spec}(S)} id) = f(S, A, \lambda) \otimes_{\mathcal{O}_S} 1 .$$

- (ii) For S -isomorphic data (A, λ) and (A', λ') one has

$$f(S, A, \lambda) = f(S, A', \lambda') .$$

Let $M_{g,R}^k$ be the space of modular forms of weight k . The direct sum over all integers k defines the graded R -algebra $M_{g,R}^\bullet = \bigoplus_k M_{g,R}^k$ of modular forms.

Variants. One has variants for the definition of modular forms: a) additional level- N -structure over extension rings R of $\mathbb{Z}[\frac{1}{N}, \zeta_N]$. This defines the stack $A_{g,R,N}$. For this we assume $2p \nmid N$ later in case R is the spectrum of a field κ of characteristic p . Or b) tensor valued modular forms, i.e. sections $f(S, A, \lambda) \in \Gamma(\text{Spec}(S), \Omega_A^{\otimes k})$ with corresponding functorial properties.

The classical case. $M_{g,\mathbb{C}}^k$ is isomorphic to the space of all holomorphic functions $f : H_g \rightarrow \mathbb{C}$ on the Siegel upper half space H_g of genus g with the property

$$f(\gamma\langle\Omega\rangle) = \det(C\Omega + D)^k f(\Omega)$$

for all $\gamma \in \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g = Sp_{2g}(\mathbb{Z})$. The isomorphism is given by

$$f \mapsto f(\Omega) = f(\mathbb{C}, \mathbb{C}/\Gamma_\Omega, \lambda_{can})$$

for periods Ω in the Siegel upper half space H_g and the standard polarization λ_{can} defined for the standard period lattice $\Gamma_\Omega = \mathbb{Z}^g + \Omega\mathbb{Z}^g$.

The Hasse invariant for $R = \mathbb{F}_p$. Let $Lie(A/S) \cong \Omega_A^*$ denote the Lie algebra of translation invariant relative vectorfields X , and let denote $D = D_X$ the derivation associated to X . Consider the Hasse-Witt map

$$\Phi : Lie(A/S) \rightarrow Lie(A/S)$$

$$\Phi(D) = D^p.$$

Notice Φ is p -linear, i.e. $\Phi(\lambda v) = \lambda^p \Phi(v)$ for $\lambda \in S$. For an arbitrary p -linear endomorphism $\Phi : V \rightarrow V$ of a locally free S -module V with $pS = 0$ put $V^{(p)} = V \otimes_S S$ such that $v\lambda \otimes_S \lambda' = v \otimes_S \lambda^p \lambda'$. Then Φ extends to a S -linear morphism $\Phi : V^{(p)} \rightarrow V$. Let $ST^p(V)$ denote the p -symmetric elements in the tensor product. It contains the symmetrization $Sym^p(\otimes^p V)$ as a S -submodule. The S -linear morphism $v \otimes \lambda \mapsto \lambda \cdot v \otimes v \otimes \cdots \otimes v$ (p copies) induces an S -isomorphism $V^{(p)} \xrightarrow{\sim} ST^p(V)/Sym^p(\otimes^p V)$ by [D], I §10. If we compose the projection

$$ST^p(V) \rightarrow ST^p(V)/Sym^p(\otimes^p V)$$

with the inverse of this isomorphism and then with Φ , we obtain a S -linear morphism $ST^p(V) \rightarrow V$. It can be considered as an element in

$$V \otimes_S S^p(V^*),$$

where $S^p(V^*)$ is the symmetric tensor quotient of the p -th tensor product of V^* defined as the quotient by the equivalence relation induced from the symmetry relations $\dots \otimes x \otimes \dots \otimes y \otimes \dots \sim \dots \otimes y \otimes \dots \otimes x \otimes \dots$

Applied for the Hasse-Witt map Φ this construction yields a sheaf homomorphism $ST^p(Lie(A/S)) \rightarrow Lie(A/S)$ or equivalently an element

$$\mathbb{A} \in \Gamma(\text{Spec}(S), S^p(\Omega_A) \otimes \Omega_A^*) .$$

Exterior powers of p -linear maps are p -linear. Hence the exterior powers $\Lambda^i(\mathbb{A})$ of \mathbb{A} define vector valued modular forms in characteristic p . In particular for $i = g$ this defines the Hasse invariant A as a modular form of weight $k = p - 1$ in the space $M_{g, \mathbb{F}_p}^{p-1}$ defined above

$$A \in \Gamma(\text{Spec}(S), \omega^{p-1}) .$$

The ungraded ring of modular forms. Assume κ to be \mathbb{F}_p or its algebraic closure $\overline{\mathbb{F}_p}$. Let denote $M_{g, \kappa}$ the associated ungraded ring of modular forms over κ obtained from the graded ring $M_{g, \kappa}^\bullet$. This ring is a normal domain. Then

Unique FaktORIZATION Theorem. *There exists a prime p_0 such that for $p > p_0$ the normal domain $M_{g, \kappa}$ of modular forms over κ is a unique factorization ring for all $g \geq 2$.*

The lemma is related to the following graded version for modular forms over κ of some level $N \geq 1$, where we tacitly assume a root of unity ζ_N to be chosen in κ .

Theorem. *For $p > p_0$ and $g \geq 3$ and $N \geq 1$ and $2p \nmid N$ the Picard group of the moduli stack $A_{g, \kappa, N}$ defined over κ is*

$$\text{Pic}(A_{g, \kappa, N}) \cong \mathbb{Z} \cdot c_1(\omega) \oplus sp_{2g}(N\mathbb{Z}/N^2\mathbb{Z}) .$$

Remark. In particular this group is of rank one, and generated by the Chern class $c_1(\omega)$ modulo a finite torsion subgroup isomorphic to the ‘Lie algebra’ $sp_{2g}(\mathbb{Z}/N\mathbb{Z})$ of the symplectic group over the ring $\mathbb{Z}/N\mathbb{Z}$. The corresponding assertion is false for $g = 2$. It does not hold for $g \geq 3$ and levels of type $N = 2^i$ either. However there are similar statements in this latter case.

Remark. To obtain the results above on Picard groups for \mathbb{F}_p it is enough to prove this over $\overline{\mathbb{F}}_p$ using descend via Hilbert theorem 90 and the vanishing of the Brauer groups of these fields.

Fourier expansion. The q -expansion of a modular form is obtained by evaluating forms at the Mumford families of principally polarized abelian varieties defined by torus quotients. The q -expansion principle [CF] gives injective maps

$$M_{g,R}^k \hookrightarrow R[[q]] := R[[q_{ij}]] \quad , \quad q_{ij} = q_{ji}, 1 \leq i, j \leq g$$

defined by

$$f \mapsto \sum_T a_f(T) q^T$$

with Fourier coefficients $a_f(T) \in R$ attached to half-integral symmetric matrices T (written as symbolic exponents). Notice, the relevant Mumford family defines an abelian scheme over $R[[q]][\frac{1}{q_{ij}}]$. Nevertheless by Koecher's effect $f \in R[[q]]$.

The theory of Chai-Faltings [CF] implies that $M_{g,\mathbb{Z}}^k = \{f \in M_{g,\mathbb{C}}^k \mid a_f(T) \in \mathbb{Z}\}$. This relates modular form over \mathbb{Z} to classical Siegel modular forms.

Example. For $R = \mathbb{F}_p$ the Hasse invariant $A \in M_{g,\mathbb{F}_p}^{p-1}$ has Fourier expansion $A = 1$. In other words $a_f(T) = 0$ for all $T \neq 0$.

We will see below that the last theorem implies

Proposition. *Assume $p > p_0$ for p_0 as in the lemma. Then the kernel of the ring homomorphism*

$$\varphi : M_{g,\mathbb{F}_p} \rightarrow \mathbb{F}_p[[q]]$$

of ungraded rings induced from the q -expansion is the principal ideal generated by $(A - 1)$ for the Hasse invariant A .

Let $S_{g,\mathbb{F}_p} \subseteq \mathbb{F}_p[[q]]$ denote the image of the homomorphism φ . It is not hard to see for $p \geq 2g + 2$ that S_{g,\mathbb{F}_p} coincides with the ring obtained by reduction mod p from the ring of the integral q -expansion of all modular forms in $M_{g,\mathbb{Z}}$. Furthermore one has the following rather obvious properties: The subring S_{g,\mathbb{F}_p} of the ring of power series $\mathbb{F}_p[[q]]$ is stable under the following operators

(1) Hecke operators $T(l)$ for primes l different from p

(2) The operators

$$U : \sum_T a(T)q^T \mapsto \sum_T a(pT)q^T$$

$$V : \sum_T a(T)q^T \mapsto \sum_T a(T)q^{pT} .$$

(3)

$$\Phi : \mathbb{F}_p[q_{11}, \dots, q_{gg}] \mapsto \mathbb{F}_p[[q_{11}, \dots, q_{g-1g-1}]]$$

$$q_{*g} = q_{g*} \mapsto 0$$

and $q_{ij} \mapsto q_{ij}$ for $i \neq g, j \neq g$. Notice

$$\Phi(S_{g, \mathbb{F}_p}) = S_{g-1, \mathbb{F}_p}$$

and

$$\Phi(M_{g, \mathbb{F}_p}) \subseteq M_{g-1, \mathbb{F}_p} .$$

For the operator V use that reduction modulo p of the normalized Hecke operator $T(p)$ coincides with V for weights $k \geq g+1$. Of course one can assume $k \geq g+1$ without restriction of generality, since multiplication with the Hasse invariant A commutes with the Hecke operators $T(l)$ for all $(l, p) = 1$. For forms f with coefficients in \mathbb{F}_p we have $f|V = f^p$.

Proof of the proposition. For the elliptic case $g = 1$ see [Sw]. The general case is reduced to the elliptic case as follows. First notice

$$\dim(S_{g, \mathbb{F}_p}) \geq \dim(M_{g, \mathbb{F}_p}) - 1 .$$

In fact, if κ is a field and $B = \bigoplus_{i=0}^{\infty} B_i$ is a finitely generated integral (graded) κ -algebra of Krull dimension $\dim(B)$, and if $\varphi : B \rightarrow S$ is a ring homomorphism onto an integral domain S such that $\varphi|_{B_i}$ is injective for every i , then $\dim(S) \geq \dim(B) - 1$. Since the stack A_{g, \mathbb{F}_p} is irreducible by a result of Chai, the graded ring of modular forms satisfies the assumptions made on B . Hence this general fact from commutative algebra can be applied for the graded ring of modular forms. Obviously $\text{Ker}(\varphi)$ is a prime ideal. Therefore it is a prime ideal of height one because the kernel is nontrivial, since $0 \neq A - 1 \in \text{Ker}(\varphi)$. Hence $\text{Ker}(\varphi)$ is a principal ideal by the unique factorization theorem stated above.

Since $A - 1$ is contained in the kernel of φ , it is enough to show that $A - 1$ is irreducible. If not $A - 1 = FG$ for $F = F_0 + \cdots + F_s$ and $G = G_0 + \cdots + G_t$ and $p - 1 = r + s$, $r > 0$, $s > 0$ and forms F_i, G_i of weight i . But then $\Phi^{g-1}(A - 1) = A - 1$ (in genus $g = 1$) implies $\Phi^{g-1}(F_s) \neq 0$ and $\Phi^{g-1}(G_t) \neq 0$ by degree reasons (notice the Hasse invariant A is nonvanishing of weight $p - 1$ for genus $g = 1$). But this factorization of $A - 1$ for genus $g = 1$ would contradict the result of Swinnerton-Dyer [Sw]. This proves the proposition. \square

By a similar argument, using the Φ -operator to reduce to the case $g = 2$, we have the following

Corollary. *For $g \geq 2$ the Hasse invariant is an irreducible modular form. In particular the locus of singular abelian varieties (the zero locus of the Hasse invariant A) is irreducible.*

For $g = 2$ this follows from results of Koblitz.

Corollary. *Suppose $g \geq 2$, $p > p_0$ and $f \in M_{g, \mathbb{F}_p}^k$. Then the following statements are equivalent*

- 1) *f is totally p -singular, i.e. $f = \sum_T a(T)q^T$ and $a(T) = 0$ unless $p|T$.*
- 2) *$f = A^r h^p$ for some $r \in \mathbb{N}_0$ and some $h \in M_{g, \mathbb{F}_p}^{k'}$.*

In particular $f = 0$ for $k < p - 1$, if one of these two equivalent conditions holds.

Proof. To show that 1) implies 2) we may assume, that A does not divide f . If f has weight k , we choose l such that $K = k + l(p - 1) \geq g + 1$. Then $A^l f$ has weight $K \geq g + 1$, hence also $(A^l f)|U$. Then $((A^l f)|U)|V = ((A^l f)|U)^p$ has weight pK , and it has the same Fourier expansion as f . Therefore $((A^l f)|U)^p = A^m f$ for $m = k + lp$ by the q -expansion principle, since both sides have the same weight and the same q -expansion. So at least the power A^{lp} divides $((A^l f)|U)^p$. Hence A^l divides $(A^l f)|U$ and $h_1 = A^{-l}(A^l f)|U$ is a modular form of weight k such that $h_1^p = A^k f$. Therefore the irreducible form A divides h_1 . In other words $h_1 = Ah_2$, hence $A^p h_2^p = A^k f$. Since A does not divide f by assumption, we conclude $h_2^p = A^{k-p} f$ and either $k = p$, or again $h_2 = Ah_3$ holds for some modular form h_2 . If we continue, this must terminate after finitely many steps. Hence k is divisible by p and there exists a modular form $h = h_\nu$ such that $h^p = f$. \square

Question. Is $S_{g, \mathbb{F}_p} \subseteq \mathbb{F}_q[[q]]$ preserved by the differential operator $\sum_T a(T) \cdot q^T \mapsto \sum_T \det(T) a(T) \cdot q^T$? Similarly is $\sum_T T \cdot a(T) q^T$ a vector valued modular form?

Proof of the theorem. For the proof we can extend the base field to become $\kappa = \overline{\mathbb{F}_p}$. Use Hilbert theorem 90 and vanishing of the Brauer group for finite fields, and later for fields of fractions of Henselian discrete valuation rings with algebraically closed residue field. We can also replace N by a suitably large integer not divisible by $2p$, so that X is a smooth variety without restriction of generality.

1) *Change of level.* Assume we are over a base scheme S over $\mathbb{Z}[\frac{1}{N}, \zeta_N]$ for $N \geq 3$. Consider the natural morphism $A_{g, S, N} \rightarrow A_{g, S}$, which is equivariant with respect to the group $G_N = Sp(2g, \mathbb{Z}/N\mathbb{Z})$. Pullback defines a natural homomorphism $Pic(A_{g, S}) \rightarrow Pic(A_{g, S, N})$. A line bundle on $A_{g, S}$ is given by its pullback \mathcal{L} on $A_{g, S, N}$ together with descent data $\varphi_\sigma : \sigma^*(\mathcal{L}) \cong \mathcal{L}$ for $\sigma \in G_N$ satisfying the obvious cocycle conditions. Since $H^0(A_{g, S, N}, \mathcal{O}^*) = \mathcal{O}_S^*(S)$ and the group G_N is perfect, the cocycle datum is uniquely determined, once it exists. Hence there exists an exact sequence

$$0 \rightarrow Pic(A_{g, S}) \rightarrow Pic(A_{g, S, N})^{G_N} \rightarrow H^2(G_N, \mathcal{O}_S^*(S))$$

For odd N and $g \geq 3$ we claim $H^2(G_N, C) = 0$ for $C = \mathcal{O}_S^*(S)$. We may replace C by an arbitrary finite trivial G_N -module. For perfect groups G the Künneth theorem and the universal coefficient theorem imply $H^2(G, C) = Hom(H_2(G, \mathbb{Z}), C)$. So it is enough to show vanishing of the Schur multiplier $M(G) = H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H_2(G, \mathbb{Z})^D$. Since the Schur multiplier is additive for products of perfect groups, one can reduce to the case where N is a prime power. According to the group Atlas, see also [FP], this Schur multiplier vanishes in the case where N is a prime different from two. Using results of [FP] one reduces this to show $H^2(G_N, \mathbb{Z}/l\mathbb{Z})$ vanishes. For $(l, N) = 1$ see [FP]. So we can assume $C = \mathbb{F}_p$. For $N = p^r$ for $r \geq 2$ and p odd now we proceed by induction on r using $G_{p^r}/Lie =: G = G_{p^{r-1}}$ with respect to the abelian group $Lie = sp_{2g}(\mathbb{Z}/p\mathbb{Z})$. The Hochschild-Serre spectral sequence and the induction assumption together with $H^0(G, H^2(Lie)) = 0$ and $H^1(G, Lie^D) = 0$ then prove the induction step. For $p \neq 2$ one has an exact sequence $0 \rightarrow Lie^D \rightarrow H^2(Lie, \mathbb{F}_p) \rightarrow \Lambda^2(Lie^D) \rightarrow 0$, hence the first statement $H^0(G, H^2(Lie)) = 0$ follows from the obvious facts $(Lie^D)^G = 0$ and $\Lambda^2(Lie^D)^G = 0$. The second assertion $H^1(G, Lie^D) = 0$ is less obvious. It follows by induction on the genus g using restriction to parabolic subgroups and standard techniques of group cohomology. Hence under our assumptions on N

the pullback defines an isomorphism

$$\boxed{Pic(A_{g,S}) \cong Pic(A_{g,S,N})^{G_N}}.$$

By the methods above one also obtains the vanishing of cohomology groups of the finite group $G_N = Sp_{2g}(\mathbb{Z}/N\mathbb{Z})$ for odd N in the following special cases

$$H^i(G_N, \mathbb{C}^*) = 0 \quad , \quad g \geq 3, i = 1, 2$$

$$H^i(G_N, (sp_{2g}(\mathbb{Z}/N\mathbb{Z}), Ad)) = 0 \quad , \quad g \geq 3, i = 0, 1 \text{ and } 2 \nmid N$$

$$H^3(G_N, \mathbb{Z})_{l-torsion} = 0 \quad , \quad \text{for } g \geq 3 \text{ and } 2 \nmid l.$$

In the proof these vanishing theorems can be used to allow the passage from level $N = 1$ to level $N > 1$ and vice versa.

2) *Analytic results over \mathbb{C} .* For $g \geq 3$ we have a) For $\Gamma_g = Sp_{2g}(\mathbb{Z})$

$$Pic(\Gamma_g) := H^1(H_g/\Gamma_g, \mathcal{O}^*(H_g)) \cong H^2(\Gamma_g, \mathbb{Z}) = \mathbb{Z} \cdot c_1(\omega) ,$$

and b) For all principal congruence subgroups $\Gamma = \Gamma_g(N)$ for $N \geq 3$

$$H^2(\Gamma, \mathbb{Z}) \cong Pic_{an}(H_g/\Gamma) \cong Pic(A_{g,\mathbb{C},N}) ,$$

and c)

$$Pic(\Gamma)_{tors} \cong (\Gamma^{ab})^D .$$

See [F], p. 257 and Hilfssatz 4. Finally d), that $Pic(\Gamma)/\mathbb{Z}c_1(\omega)$ is a finite group for $g \geq 3$ and arbitrary subgroups Γ of finite index in Γ_g . This follows from theorems of A. Borel and vanishing theorems (resp. L^2 -vanishing theorems for $g = 3$) for Lie algebra cohomology.

Recall $G_N = \Gamma_g/\Gamma_g(N)$. By step 1 the E_2 -term of the Hochschild-Serre spectral sequence $H^i(G_N, H^j(\Gamma_g(N), \mathbb{Z})) \implies H^{i+j}(\Gamma_g)$ for $i + j = 2$ has only $H^0(G_N, H^2(\Gamma_g(N), \mathbb{Z}))$ as nontrivial summand, and degenerates in this degree at the E_3 -term, i.e. the differential d_3 induces a canonical exact sequence

$$0 \rightarrow H^2(\Gamma_g, \mathbb{Z}) \rightarrow H^2(\Gamma_g(N), \mathbb{Z})^{\Gamma_g} \rightarrow H^3(G_N, \mathbb{Z}) .$$

Since $H^3(G_N, \mathbb{Z}) \cong H^2(G_N, \mathbb{Q}/\mathbb{Z})$ the vanishing of Schur multiplier explained in step 1 implies $H^3(G_N, \mathbb{Z}) = 0$ for odd N and $g \geq 3$. Hence the restriction map induces a canonical isomorphism

$$\boxed{res : H^2(\Gamma_g, \mathbb{Z}) \cong H^2(\Gamma_g(N), \mathbb{Z})^{\Gamma_g}}$$

for $g \geq 3$ and odd integers N . Hence both for the stack setting as well as for the analytic setting the descend from level N to level one only amounts to consider G_N -invariants. This is used in step 4) below.

A first application of this descend principle: For $N \geq 3$ and $g \geq 3$ the long exact sequence of G_N -invariants for the exact sequence $0 \rightarrow (\Gamma^{ab})^D \rightarrow \text{Pic}(A_{g,\mathbb{C},N}) \xrightarrow{p} \mathbb{Z} \rightarrow 0$ from assertion 2c) and 2d) and the vanishing of the cohomology groups $H^i(G_N, (\Gamma^{ab})^D) = 0$ for $i = 0, 1$ implies that p induces an isomorphism $p : \text{Pic}(A_{g,\mathbb{C},N}) \cong \mathbb{Z}$. Here we used $\Gamma_g(N)^{ab} = \Gamma_g(N)/\Gamma_g(2N) \cong \text{sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ and the vanishing theorems of step 1, in particular that the perfect group G_N acts trivially on the cyclic quotient group \mathbb{Z} . The descend principle above thus gives the canonical isomorphism

$$p : \text{Pic}(A_{g,\mathbb{C}}) \cong \mathbb{Z}.$$

Since $c_1(\omega)$ generates $\text{Pic}(A_{g,\mathbb{C}}) \cong H^2(\Gamma_g, \mathbb{Z})$ by 2b) we conclude that the projection map p induces an isomorphism

$$\text{Pic}(A_{g,\mathbb{C},N}) \cong \mathbb{Z} \cdot c_1(\omega) \oplus \text{Pic}(A_{g,\mathbb{C},N})_{\text{tors}}$$

for odd N and $g \geq 3$. We would like to carry this over to the Picard groups of $A_{g,\mathbb{F}_p,N}$ via smooth and proper base change for etale l -adic cohomology for all $l \neq p$. For this consider $N \geq 3$ and compactifications.

3) *Passage to compactification.* There exists an exact G_N -equivariant sequence

$$0 \rightarrow \mathbb{Z}^r \rightarrow \text{Pic}(\overline{A_{g,\kappa,N}}) \rightarrow \text{Pic}(A_{g,\kappa,N}) \rightarrow 0$$

for suitable toroidal compactification $\overline{A_{g,\kappa,N}}$ of $A_{g,\kappa,N}$ in the sense of Chai-Faltings. Indeed the subgroup generated by the boundary divisors is torsion-free by Koecher's principle, hence isomorphic to \mathbb{Z}^r for a suitable integer r depending on N, g and the compactification. The same sequences exist over $\mathbb{Z}[\frac{1}{N}, \zeta_N]$ and \mathbb{C} .

4) *Base change.* The strategy of proof is to reduce the assertion of the theorem to the case of level $N = 1$ using step 1). For $N = 1$ we have to show $\text{Pic}(A_{g,\kappa}) = \mathbb{Z} \cdot c_1(\omega)$. For this choose some auxiliary prime l different from p , and first show $\text{Pic}(A_{g,\kappa}) \otimes \mathbb{Z}_l = \mathbb{Z}_l \cdot c_1(\omega)$. If the stack A_g were a smooth and proper scheme, this could be easily deduced from the analytic facts stated in 2) by proper and smooth base change. Since it is not one has to pass to some larger level N and consider a toroidal compactification for which it is possible to apply the smooth

and proper base change theorem. Using step 1) and 3) one can pass back to derive $Pic(A_{g,\kappa}) \otimes \mathbb{Z}_l = \mathbb{Z}_l \cdot c_1(\omega)$. For varying l this implies that $Pic(A_{g,\kappa})/(\mathbb{Z} \cdot c_1(\omega))$ is a finite p -primary abelian group.

To make this outline more precise choose an integer l prime to p . One can assume $N \geq 3$. First one replaces \mathbb{F}_p by its algebraic closure $\overline{\mathbb{F}}_p$. Apply the snake lemma to the exact sequences of step 3 with respect to multiplication by l . This gives a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & Pic(\overline{X}/\kappa)[l] & \longrightarrow & Pic(A_{g,\kappa,N})[l] & \longrightarrow & (\mathbb{Z}/l\mathbb{Z})^r \longrightarrow Pic(\overline{X}/\kappa)/l \\ & & \downarrow & & \downarrow & & \parallel \\ 0 & \longrightarrow & Pic(\overline{X}/\mathbb{C})[l] & \longrightarrow & Pic(A_{g,\mathbb{C},N})[l] & \longrightarrow & (\mathbb{Z}/l\mathbb{Z})^r \longrightarrow Pic(\overline{X}/\mathbb{C})/l \end{array}$$

for toroidal compactifications \overline{X} as in step 3. Notice $Pic(\overline{X}/\kappa) \cong H^1(\overline{X}/\kappa, \mu_l)$ for $\kappa = \overline{\mathbb{F}}_p$ and $\kappa = \mathbb{C}$. Hence the left vertical arrow is an isomorphism by the proper smooth etale base change theorem. This implies that the second vertical specialization map is injective. Next notice that the abelian variety $Pic^0(\overline{X}/\kappa)$ vanishes. Look at m -torsion points for large auxiliary integers m prime to p . Then $Pic^0(\overline{X}/\kappa)$ is a group of type $(\mathbb{Z}/m\mathbb{Z})^{2d}$. As a subgroup of $Pic(\overline{X}/\kappa)$ this forces $d = 0$. To show this use base change for the first etale cohomology to reduce this to the case $\kappa = \mathbb{C}$, where this immediately follows from step 2). The vanishing of $Pic^0(\overline{X}/\kappa)$ implies $Pic(\overline{X}/\kappa) = NS(\overline{X}/\kappa)$. By the Kummer sequence one has inclusions $Pic(\overline{X}/\kappa)/l \hookrightarrow H_{et}^2(\overline{X}/\kappa, \mu_l)$ respectively canonical inclusions $Pic(\overline{X}/\overline{\mathbb{F}}_p) \otimes \mathbb{Z}_l \hookrightarrow H_{et}^2(\overline{X}/\mathbb{C}, \mathbb{Z}_l)$ for prime l . By base change $H_{et}^2(\overline{X}/\overline{\mathbb{F}}_p, \mu_l) \cong H_{et}^2(\overline{X}/\mathbb{C}, \mu_l)$ respectively $H_{et}^2(\overline{X}/\overline{\mathbb{F}}_p, \mathbb{Z}_l) \cong H_{et}^2(\overline{X}/\mathbb{C}, \mathbb{Z}_l)$. Furthermore $H_{et}^2(\overline{X}/\mathbb{C}, \mathbb{Z}_l) \cong H_{et}^2(\overline{X}/\mathbb{C}, \mathbb{Z}) \otimes \mathbb{Z}_l$. Hence the smooth and proper base change theorem implies that the fourth vertical map of the diagram above is injective. This implies by the 5-lemma, that the second vertical map also is surjective. Hence the second vertical map is an isomorphism

$$Pic(A_{g,\overline{\mathbb{F}}_p,N})[l] \cong Pic(A_{g,\mathbb{C},N})[l] .$$

The argument also gives an injective map

$$Pic(A_{g,\overline{\mathbb{F}}_p,N})/l \hookrightarrow Pic(A_{g,\mathbb{C},N})/l .$$

Together this implies the analog of assertion 2d) over $\overline{\mathbb{F}}_p$. Hence

$$Pic(A_{g,\overline{\mathbb{F}}_p,N})/Pic(A_{g,\overline{\mathbb{F}}_p,N})_{tors} \cong \mathbb{Z} .$$

Since $Pic(A_{g,\overline{\mathbb{F}}_p,N})_{tors}$ is $(\Gamma_g(N)^{ab})^D$ up to p -power torsion as shown above, by taking G_N -invariants the argument at the end of step 2 give the following result

$$Pic(A_{g,\mathbb{C},N}) \otimes \mathbb{Z}_l \cong (\mathbb{Z}_l \cdot c_1(\omega)) \oplus (\mathbb{Z}_l \otimes Pic(A_{g,\mathbb{C},N})_{tors}) .$$

for all primes l different from p . Warning: Usually taking invariants does not commutes with the tensor product with \mathbb{Z}_l . Here it does by a simple inspection.

5) *p-index*. To control the cotorsion of the subgroup generated by $c_1(\omega)$ in the group $Pic(A_{g,\mathbb{F}_p,N})$ for $N = 1$ one suitably embeds $A_{2,\mathbb{F}_p} \hookrightarrow A_{g,\mathbb{F}_p}$ such that ω pulls back to ω . Suppose $\mathcal{L}^e = \omega$ for a line bundle \mathcal{L} on A_{g,\mathbb{F}_p} . Then of course the same holds for the pullback of \mathcal{L} to A_{2,\mathbb{F}_p} . So this reduces us to consider the case $g = 2$ for this question. Now Igusa [I] has given an explicit description of the coarse moduli space A_2^{coarse} of the stack A_2 . In fact for $p \neq 2, 3$ the space $A_{2,\mathbb{F}_p}^{coarse}$ is a quotient U/G , where U is the open complement of some closed subset of codimension 2 in the projective space \mathbb{P}^3 , and where G is the finite group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ acting on U . The same holds over $\kappa = \overline{\mathbb{F}}_p$. Consider

$$\begin{array}{ccc} & A_{2,\overline{\mathbb{F}}_p,3} & \\ \swarrow & & \searrow \\ A_{2,\overline{\mathbb{F}}_p} & & A_{2,\overline{\mathbb{F}}_p}^{coarse} \end{array} .$$

A suitable power of ω^r descends to $A_{2,\overline{\mathbb{F}}_p}^{coarse}$. Since the Picard group of U is cyclic, this provides an a priori bound e_0 for the integer e independent from g and p . Since on the other hand e must be a power of p by step 4) we find that for large enough $p > p_0$ necessarily $e = 1$ holds. This proves $Pic(A_{g,\overline{\mathbb{F}}_p}) = \mathbb{Z}c_1(\omega) \oplus T$ for a finite p -primary torsion group T .

6) *p-torsion*. To show that the torsion T vanishes it is enough to control the p -torsion $Pic(A_{g,\kappa})[p]$. For this we may pass to a suitably large level N not divisible by $2p$. Then the covering space $X = A_{g,\kappa,N}$ is smooth. It is enough to show $Pic(X)[p] = 0$. In general, for smooth X over κ one can control $Pic(X)[p] = 0$ by the closed 1-forms on X . In fact, if C denotes the Cartier operator, then one has a surjection

$$\left\{ \eta \in H^0(X, \Omega_X^1) \mid d\eta = 0, C\eta = \eta \right\} \cong H^1(X_{flat}, \mu_p) \twoheadrightarrow Pic(X)[p] .$$

Hence to show that $Pic(X)[p]$ vanishes under the assumptions made, it is enough to proof the following

Vanishing Theorem. *Suppose $g \geq 2$ and $p \neq 2$ and let κ be $\mathbb{F}_p[\zeta_N]$ or $\overline{\mathbb{F}}_p$. Then for $X = A_{g,\kappa,N}$ and arbitrary level N not divisible by p the following holds*

$$H^0(X, \Omega_X^1) = 0 .$$

Remark. The proof of this vanishing theorem can be extended to the case of regular alternating differential forms Ω_X^i on X of degree i for $i < \frac{g}{2}$ and $i < \frac{p-1}{2}$.

Remark. We could compute p_0 from step 5 of the above proof of the theorem and the assumption $p \neq 2$.

Proof of the vanishing theorem. The proof proceeds by induction on g . In some sense the case $g = 2$ is the most complicated case. For the proof we can choose some embedding $\mathbb{Z}[\zeta_N]$ to $\overline{\mathbb{F}}_p$ and extend the base field κ to become $\overline{\mathbb{F}}_p$. We can also replace N by a suitably large integer not divisible by p , so that X is a smooth variety without restriction of generality.

a) *q-expansion.* As a first step in the proof use that any regular 1-form η on $A_{g,\mathbb{F}_p,N}$ automatically extends to a 1-form $\eta \in \Omega_{\overline{X}}^1(log)$ with log-poles on the toroidal compactification $\overline{X} = \overline{A_{g,\kappa,N}}$ (Koecher's principle). Furthermore notice the Kodaira-Spencer isomorphism in the sense of [CF], p.107

$$\Omega_{\overline{X}}^1(log) \cong S^2(\Omega_A) .$$

In other words, one can expand η in the following form using q -expansion

$$\eta = \sum_{T \geq 0} \text{Trace}(a(T) \cdot d\log(q)) \cdot q^T ,$$

where $a(T)$ is a symmetric g by g matrix with coefficients in κ and where T runs over the halfintegral semidefinite g by g matrices (notation is chosen to hide N). E.g. for $g = 2$

$$d\log(q) = \begin{pmatrix} \frac{dq_{11}}{q_{11}} & \frac{dq_{12}}{q_{12}} \\ \frac{dq_{21}}{q_{21}} & \frac{dq_{22}}{q_{22}} \end{pmatrix} .$$

b) *Equivariance.* For unimodular $U \in Gl(g, \mathbb{Z})$ congruent to id modulo N with image \bar{U} in $Gl(g, \mathbb{Z}/p\mathbb{Z})$ the Fourier coefficients $a(T)$ of the 1-form η satisfy

$$(*) \quad \boxed{a({}^tUTU) = {}^t\bar{U}a(T)\bar{U}}.$$

In particular $a(0) = 0$.

c) *Cartier operator.* Suppose there exists a 1-form $\eta \neq 0$ on X . Without restriction of generality one can choose η such that there exists T with $a(T) \neq 0$ and $p \nmid T$. Notice otherwise the form is closed, so one can apply the Cartier operator $C : \Omega_{X, closed}^1 \rightarrow \Omega_{X^{(p)}}^1$. Since $C(\sum_T a(T)q^T d\log(q)) = \sum_T \tilde{a}(T)q^{T/p} d\log(q)$, this process terminates after finitely many steps and gives the desired form η on $X^{(p^s)}$. We may replace $X^{(p^s)}$ by X , since this amounts just to another choice of $\zeta_N \in \kappa$. By b) we can in addition assume $T = \begin{pmatrix} * & * \\ * & \nu \end{pmatrix}$ with last entry $T_{gg} = \nu \not\equiv 0 \pmod{p}$.

d) *A boundary chart.* For the sake of simplicity temporarily assume $N = 1$. Let

$$\pi : \mathcal{A}_{g-1} \rightarrow \mathcal{A}_{g-1}$$

be the universal abelian scheme with polarization $\lambda : \mathcal{A}_{g-1} \rightarrow \mathcal{A}_{g-1}^\vee$. On the pullback $\Xi = \Xi_\xi = j^*(\mathcal{P}^{-1})$ of the Poincare \mathbb{G}_m -torsor \mathcal{P} over $\mathcal{A}_{g-1} \times_{\mathcal{A}_{g-1}} \mathcal{A}_{g-1}^\vee$ under $j = id \times \lambda$ the group \mathbb{G}_m acts such that the canonical map $u : \Xi \rightarrow \mathcal{A}_{g-1}$ induces an isomorphism $\Xi/\mathbb{G}_m \cong \mathcal{A}_{g-1}$. A formal boundary chart $S = S_\xi$ of the toroidal compactification is now obtained by the formal completion of $\bar{\Xi} = (\Xi \times \mathbb{A}^1)/\mathbb{G}_m$ along the zero section. Indeed

$$u : \bar{\Xi} \rightarrow \mathcal{A}_{g-1}$$

is a line bundle over \mathcal{A}_{g-1} . The complement of the zero section is the \mathbb{G}_m -bundle $\Xi = (\Xi \times \mathbb{G}_m)/\mathbb{G}_m$ we started from. See [CH], p.104 ff for $X_\xi = \mathbb{Z}$, $E_\xi = \mathbb{G}_m$ and $E_\xi = \mathbb{A}^1$.

e) *Fourier-Jacobi expansion.* Then η , considered as a differential form on S with log-poles, can be expanded $u_*(\eta|_S) = \sum_\nu u_*(\eta)^{\chi_\nu} q^\nu$ with respect to the characters $\chi_\nu(t) = t^\nu$ of \mathbb{G}_m . Here $q \in \Gamma(\bar{\Xi}, \mathcal{L}_0^{-1})$ is the tautological section for $\mathcal{L}_0 = (id \times \lambda)^*(\mathcal{P})$. Notice $q = \tau(\chi_1, \chi_1)$ in the notation of [CF], p.106. To relate this to the Fourier-Jacobi expansion one needs to consider the semiabelian principally polarized scheme ${}^\heartsuit G$ defined over S by Mumford's construction. It contains a split torus T over S of rank one with the abelian scheme

quotient ${}^\heartsuit G/T \cong \mathcal{A}_{g-1}$. Notice $\Omega_T \cong \mathcal{O}_S$ via $\frac{dq}{q} \mapsto 1$. The exact sequence $0 \rightarrow \Omega_{\mathcal{A}_{g-1}} \rightarrow \Omega_{{}^\heartsuit G} \rightarrow \Omega_T \rightarrow 0$ of relative differential forms over S and the Kodaira-Spencer isomorphism $\text{Sym}^2(\Omega_{{}^\heartsuit G}) \cong \Omega^1(\log)$ give rise to an isomorphism $\Omega_S^1 = u^*(\mathcal{E})$ for a vector bundle \mathcal{E} on \mathcal{A}_{g-1} , which is pinched into an exact sequence

$$0 \rightarrow \Omega_{\mathcal{A}_{g-1}}^1 \rightarrow \mathcal{E} \xrightarrow{r} \mathcal{O}_{\mathcal{A}_{g-1}} \rightarrow 0.$$

The coefficients $u_*(\eta)^\chi$ are global sections of $u_*(u^*(\mathcal{E}))^\chi = \mathcal{E} \otimes_{\mathcal{O}_{\mathcal{A}_{g-1}}} u_*(\mathcal{O}_S)^\chi$.

Separability. Notice $u_*(\mathcal{O}_S)^\chi = \mathcal{L}_0^\nu$, where $\mathcal{L}_0 = (id \times \lambda)^*(\mathcal{P})$ is a totally symmetric line bundle on \mathcal{A}_{g-1} normalized along the zero section. Recall $p \neq 2$. Hence for

$$\nu \not\equiv 0 \pmod{p}$$

the line bundle $\mathcal{L} = \mathcal{L}_0^\nu$ is separable over the base $A_{g-1,\kappa}$ of characteristic p . This allows to relate the sections of $u_*(\mathcal{O})^\chi$ to theta functions. This will be explained in the next section. Indeed on some etale extension S of the base (e.g. $S = A_{g-1,\kappa,2\nu}$) the line bundle \mathcal{L} is of type $\delta = (2\nu, \dots, 2\nu)$ in the sense of Mumford (see also the next section). By further increasing the level we will see that then $(\mathcal{A}_{g-1}, \pi, \mathcal{L})$ admits a δ -marking in the following sense.

f) *Theta functions.* For an abelian scheme $\mathcal{A} \rightarrow S$ of relative dimension g and a totally symmetric relative ample line bundle \mathcal{L} on \mathcal{A} normalized along the zero section Mumford defined the theta group scheme $\mathcal{G}(\mathcal{L})$ over S ([M2], prop 1). For a type $\delta = (d_1, \dots, d_g)$ of even integers with $d_i | d_{i+1}$ for all i one also has the Heisenberg group scheme $\mathcal{G}(\delta)$ over S as defined in [M2], p.77. Here, as in [M2], we will suppose a separability condition, namely that $d = \prod_{i=1}^g d_i$ is invertible on the base scheme S . Then by definition a symmetric ϑ -structure, or δ -marking, for $(\mathcal{A}, \pi, \mathcal{L})$ is an isomorphism $\mathcal{G}(\mathcal{L}) \cong \mathcal{G}(\delta)$ with some additional compatibility properties as defined in [M2], p.79. Let $V(\delta)$ be the free $\mathbb{Z}[d^{-1}]$ -module generated of functions $K(\delta) = \bigoplus_i (\mathbb{Z}/d_i\mathbb{Z}) \rightarrow \mathbb{Z}[d^{-1}]$. Then [M2] prop. 2 and the discussion in loc. cit p.81 implies for a given δ -marking that there exists an equivariant isomorphism of \mathcal{O}_S -sheaves

$$\alpha : V_\delta \otimes_{\mathbb{Z}} K \cong \pi_*(\mathcal{L})$$

for some invertible sheaf K on S , unique up to multiplication with some unit in $\mathcal{O}^*(S)$. Furthermore [CF], theorem 5.1 gives $K^{8d^4} \otimes \omega^{4d^4} \cong \mathcal{O}_S$, since $\det(\pi_*(\mathcal{L})) = K^d$ for $d = (2\nu)^g$. Hence $K^2 \otimes \omega$ is a torsion line bundle on S killed by $4d^4$. We

notice, that Mumford's theory of theta functions also gives an injections

$$K \hookrightarrow \mathcal{O}_S .$$

Additional remark. Suppose $g \geq 3$. By suitably extending the level N to large N' , but still with $(N', p) = 1$, all torsion line bundles in $\text{Pic}(S)[4d^4]$ become trivial over $A_{g-1, \kappa, N'}$. For $g \geq 3$ this is first shown over \mathbb{C} , but then follows by the methods used for the proof of the theorem. Alternative argument (for all $g \geq 1$). Use that K is defined over $\mathbb{Z}[\frac{1}{2\nu}, \zeta_{N'}]$. Since the characteristic p fiber of $A_{g, \kappa, N'}$ is irreducible for $(N', p) = 1$, hence a principal divisor, one can reduce the statement to characteristic zero, where this can be explicitly computed by cocycles.

g) *Existence of δ -markings.* In the case of base fields existence of δ -markings for a given symplectic isomorphism $g_2 : H(\mathcal{L}^2) \cong H(2\delta)$ is shown in [M] §2 (remark 3, p. 319). Such a symplectic isomorphism g_2 exists over $S = A_{g-1, \kappa, N}$ by extending the level N . It is enough that 4ν divides the level N . For a general base S , different to the case of a base field considered in loc. cit., there exists an obstruction to lifting g_2 to a symmetric isomorphism $f_2 : \mathcal{G}(\mathcal{L}^2) \rightarrow \mathcal{G}(2\delta)$. The proof of loc. cit. carries over, if this obstruction vanishes. The obstruction is defined by the map

$$\delta : \mathcal{H}(\mathcal{L}^2) \rightarrow \text{Pic}(S)[8\nu]$$

given by $\delta(s) = t_{s*}(\mathcal{L}^2) \otimes \mathcal{L}^{-2}$ for sections $s : S \rightarrow \mathcal{H}(\mathcal{L}^2)$. This map is quadratic by the theorem of cube and 'pointe de degree 2' in the sense of [MB], p.12. Indeed $\delta(rs) = r^2\delta(s)$ for all $r \in \mathbb{N}$, since \mathcal{L} is symmetric. If m annihilates $\mathcal{H}(\mathcal{L}^2)$ the values of δ are m -torsion (resp $2m$ -torsion if $2|m$) line bundles on S by [MB], lemma 5.6. In our case this applies for $m = 4\nu$. If we extend the base to level $2m^2$, then every $s \in \mathcal{H}(\mathcal{L}^2)$ can be written in the form $s = 2my$. But $\delta(s) = \delta(2my) = 4m^2\delta(y)$. Since $\delta(y)$ is $4m^2$ -torsion, we get $\delta(s) = 0$. Hence a δ -marking exists after a suitable choice of level, i.e. after an etale extension of our base scheme $S = A_{g-1, \kappa, N}$.

h) *The induction step.* Suppose $g \geq 3$. To show $\Omega^1(X) = 0$ it suffices to prove $u_*(\eta)^\chi = 0$ for all $\chi(t) = t^\nu$ with $\nu \geq 0$ and $\nu \not\equiv 0 \pmod{p}$ by step e) and f). Indeed the Fourier-Jacobi expansion corresponds to the expansion with respect to the parameter $q = q_{gg}$. So it is enough to show $\Gamma(\mathcal{A}_{g-1}, \mathcal{E} \otimes \mathcal{L})$ for the separable invertible sheaves $\mathcal{L} = \mathcal{L}_0^\nu$. Using the exact sequence for \mathcal{E} and the sequence $0 \rightarrow \Omega_X^1 \rightarrow \Omega_{\mathcal{A}_{g-1}}^1 \rightarrow \Omega_A \rightarrow 0$ for $A = \mathcal{A}_{g-1}$ over S it suffices to show for $X =$

$A_{g-1,\kappa,N}$ the vanishing $\Gamma(X, K) = 0$, $\Gamma(X, \Omega_A \otimes K) = 0$ and $\Gamma(X, \Omega_X^1 \otimes K) = 0$. By $K \hookrightarrow \mathcal{O}_X$ and by the Kodaira-Spencer isomorphism the last two statements are reduced to the induction assumption $\Gamma(X, \Omega_X^1) = 0$ in genus $g-1$. This proves the induction step, since obviously $\Gamma(X, K) = 0$.

i) *Start of induction.* We now consider the case $g = 2$. Here the argument of step h) fails, since the space of 1-forms in genus one usually is nontrivial. However in the situation as in h) the argument implies that under the projection $r : \mathcal{E} \otimes \mathcal{L} \rightarrow \mathcal{L}$

$$r(u_*(\eta)^\chi) \in \Gamma(\mathcal{A}_{g-1}, \mathcal{L})$$

vanishes. Indeed, this is a section in $\Gamma(\mathcal{A}_{g-1}, \mathcal{L}) \cong \Gamma(X, \pi_*(\mathcal{L}))$. Let us consider its Fourier expansion. One can easily reduce to consider the standard cusp at infinity by replacing η without changing the condition obtained by c). By the Koecher effect applied for η this expansion is holomorphic at the cusp. Hence $r(u_*(\eta)^\chi)$ vanishes, since a power of it is a modular form of negative weight. Now this implies that all $f(q_{11}, q_{12})q_{22}^\nu \cdot \frac{dq_{22}}{q_{22}}$ terms in the Fourier expansion of η vanish for $\nu \not\equiv 0 \pmod p$. In other words

$$(**) \quad \boxed{{}^t\overline{v}\overline{T}\overline{v} \neq 0 \text{ for } \overline{v} \in \mathbb{F}_p^g \implies {}^t\overline{v}a(T)\overline{v} = 0}.$$

In fact by step b) it is enough to have this for ${}^t\overline{v} = (0, 1)$, since in general ${}^tv = (0, 1){}^tU$ for some unimodular matrix U congruent to $id \pmod N$.

j) Suppose $\det(T) \not\equiv 0 \pmod p$. Then the reduction \overline{T} of $T \pmod p$ is a nondegenerate binary quadratic form over \mathbb{F}_p . Also $S = a(T)$ is a binary quadratic form, and it is easy to see that (**) then implies $S = 0$. Also $a(0) = 0$ by step b), hence $a(T)$ vanishes unless the reduction \overline{T} of $T \pmod p$ has rank 1 with coefficient $\nu = \overline{T}_{22} \neq 0$ in $\mathbb{F}_p \subseteq \kappa$. Then necessarily

$$\overline{T} = \begin{pmatrix} x^2\nu & x\nu \\ x\nu & \nu \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \nu \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

for some $x \in \mathbb{F}_p \subseteq \kappa$.

k) *Fourier-Jacobi expansion revisited.* We now compare the Fourier expansion of $\eta \in \Omega^1(X)$ with its Fourier-Jacobi expansion for $q = q_{22}$. To unburden notation let us assume level $N = 1$ for simplicity. Then

$$\eta = \sum_{\nu=0}^{\infty} \eta_\nu(q_{11}, q_{12}) q_{22}^\nu,$$

where $\eta_\nu = \sum A \begin{pmatrix} t_0 & t_1 \\ t_1 & \nu \end{pmatrix} q_{11}^{t_0} q_{12}^{2t_1}$ with summation over semidefinite matrices $\begin{pmatrix} t_0 & t_1 \\ t_1 & \nu \end{pmatrix}$ with $t_0 \in \mathbb{Z}$ and $2t_1 \in \mathbb{Z}$. Using the transformation property b) for $U = \begin{pmatrix} 1 & 0 \\ g & 1 \end{pmatrix}$ with $g \in \mathbb{Z}$ we can also write

$$\eta_\nu(q_{11}, q_{12}) = \sum_a \left(\sum_{t_0} \vartheta_a^{A(t_0)} \cdot q_{11}^{t_0 - \frac{a^2}{4\nu}} \right)$$

where now a runs over the finitely many cosets $a \in \frac{1}{2}\mathbb{Z}^{g-1}/\nu\mathbb{Z}^{g-1}$, and where t_0 runs over all integers $t_0 \geq \frac{a^2}{4\nu}$. Notice that $A(t_0) = \begin{pmatrix} t_0 & a \\ a & \nu \end{pmatrix}$ depends on t_0 . Here we used for an integral matrix 2×2 -matrix $A = \begin{pmatrix} a_0 & a_1 \\ a_1 & a_2 \end{pmatrix}$ (or its reduction mod p) the notation

$$\begin{aligned} \vartheta_a^A &= \sum_{g \in \mathbb{Z}} \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & 0 \\ g & 1 \end{pmatrix} \cdot q_{11}^{\nu(g + \frac{a}{\nu})^2} q_{12}^{2\nu(g + \frac{a}{\nu})} \\ &= \sum_{g \in \mathbb{Z}} \begin{pmatrix} a_0 + 2ga_1 + g^2a_2 & a_1 + ga_2 \\ a_1 + ga_2 & a_2 \end{pmatrix} \cdot q_{11}^{\nu(g + \frac{a}{\nu})^2} q_{12}^{2\nu(g + \frac{a}{\nu})} \\ &= \begin{pmatrix} a_0 & a_1 \\ a_1 & a_2 \end{pmatrix} f_a + \begin{pmatrix} 2a_1 & a_2 \\ a_2 & 0 \end{pmatrix} f_a^{(1)} + \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix} f_a^{(2)} \end{aligned}$$

for the derivatives $f_a^{(i)} = \sum_{g \in \mathbb{Z}} g^i q_{11}^{\nu(g + \frac{a}{\nu})^2} q_{12}^{2\nu(g + \frac{a}{\nu})}$ of the theta functions $f_a(q_{11}, q_{12})$. Summation over t_0 therefore expresses $\eta_\nu(q_{11}, q_{12})$ as a sum over a of terms of the form

$$\begin{aligned} &f_a \cdot \left(g_{0,a} \frac{dq_{11}}{q_{11}} + 2g_{1,a} \frac{dq_{12}}{q_{12}} + g_{2,a} \frac{dq_{22}}{q_{22}} \right) + \\ &f_a^{(1)} \cdot \left(2g_{1,a} \frac{dq_{11}}{q_{11}} + 2g_{2,a} \frac{dq_{12}}{q_{12}} \right) + f_a^{(2)} \cdot g_{2,a} \frac{dq_{11}}{q_{11}} \end{aligned}$$

for power series $g_{i,a} = g_{i,a}(q_{11})$ in the variable q_{11} . Linear independency of the theta functions f_a (Mumford's theory) and step i) imply

$$g_{2,a}(q_{11}) = 0$$

by looking at the coefficient at $\frac{dq}{q} = \frac{dq_{22}}{q_{22}}$. Hence the terms simplify to

$$f_a \cdot \left(g_{0,a} \frac{dq_{11}}{q_{11}} + 2g_{1,a} \frac{dq_{12}}{q_{12}} \right) + f_a^{(1)} \cdot 2g_{1,a} \frac{dq_{11}}{q_{11}}.$$

The coefficients $g_{1,a}$ are sections in $\Gamma(A_{1,\kappa,n}, \Omega_{A_{1,\kappa,n}} \otimes K^{-1})$ and the coefficients $g_{0,a}$ are sections in $\Gamma(A_{1,\kappa,n}, \Omega_{A_{1,\kappa,n}}^1 \otimes K^{-1})$ for suitably levels n as in step h). For

the choice of n see step f) and g). Morally speaking $g_{1,a}, g_{0,a}$ are modular forms of genus one of level n and weight $\frac{1}{2}$ respectively $\frac{3}{2}$, if this is suitably defined via theta line bundles. By the way they arise it is easy to see, that they are holomorphic at the cusps.

l) *p-singularity*. Notice the Fourier coefficients of $\vartheta^{A(t_0)} q_{22}''$ are all of the form

$$T' = \begin{pmatrix} \nu y^2 & \nu y \\ \nu y & \nu \end{pmatrix}$$

where $y \in \frac{1}{M}\mathbb{Z}$ for some integer M with $(M, p) = 1$. Notice M also takes care of the level N , which was suppressed so far. Looking at the Fourier coefficients of $\frac{dq_{12}}{q_{12}}$ in the q -expansion of η only those T contribute with $T = T' + \begin{pmatrix} l & 0 \\ 0 & 0 \end{pmatrix}$, where l comes from the Fourier expansion of the section $g_{1,a}(q_{11})$. Reading this modulo p by step j) gives

$$\begin{pmatrix} \nu x^2 & \nu x \\ \nu x & \nu \end{pmatrix} \equiv \begin{pmatrix} \nu y^2 & \nu y \\ \nu y & \nu \end{pmatrix} + \begin{pmatrix} l & 0 \\ 0 & 0 \end{pmatrix}$$

modulo p , since $\nu \not\equiv 0 \pmod{p}$. Hence x and y are congruent modulo p , and therefore

$$l \equiv 0 \pmod{p}.$$

This implies that the q_{11} -expansions of the sections $g_{1,a}$ are p -singular for all a . Using this consider the $\frac{dq_{11}}{g_{11}}$ term. From the linear independency of the f_a then the same also follows for the $g_{0,a}$. In other words

$$g_{i,a}(q_{11}) = \sum_{n \geq 0} c_{i,a,n} \cdot q_{11}^{n/M}, \quad c_{i,a,n} = 0 \text{ if } p \nmid n.$$

m) *Vanishing of the $g_{i,a}$* . Since $(g_{i,a})^2$ are modular forms of weight 1 resp. 3 of genus one with suitable level n in the sense of Katz [K2] by step k), the p -singularity shown in step l) contradicts corollary (2) of the theorem of loc. cit, p.55 unless $(g_{i,a})^2 = 0$ since 1 resp. 3 is $< p - 1$ by our assumption $p \neq 2, 3$. This theorem of Katz is a version in the elliptic case with level structure of part 2) of our second corollary above. We conclude $g_{i,a} = 0$ for all i , hence $\eta = 0$. This proves the vanishing theorem for $p \neq 2, 3$. For $p = 3$ we only have $g_{1,a} = 0$. But this implies, that all Fourier coefficients $A(T)$ for matrices T with $T_{22} \not\equiv 0 \pmod{3}$ have coefficients $A(T)_{ij} = 0$ unless $i = 1, j = 1$. But this implies $A(T) = 0$ for all such Fourier coefficients by the transformation property (*). By j) it is enough to

suppose $\overline{T} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Then otherwise up to a constant $A(T) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Now apply U with $\overline{U} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Then we get $\overline{T}_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $A(T_1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ from (*). A contradiction to (**). This proves the theorem for $p = 3$. \square

Proof of the unique factorization theorem. We may suppose $g \geq 3$, since for $g = 2$ the assertion follows from [I]. Let $R_N = M_{g,\kappa,N}$ denote the ungraded ring of modular form of level g with level- N -structure. We have to show that the class group $Cl(R_N)$ of the Krull domain $R_N = M_{g,\kappa,N}$ vanishes for level $N = 1$. For suitably high level N (divisible by 8) there exists a projective embedding $\phi : A_{g,\kappa,N}^* \hookrightarrow \mathbb{P}$ of the minimal compactification $X^* = A_{g,\kappa,N}^*$ of $X = A_{g,\kappa,N}$ into projective space by the theory of theta functions, such that $j^*(\mathcal{O}_{\mathbb{P}}(1)) = \omega$. See [CF], p.157-159 and [CF], V.5. (It is preferable to use theta-level-structures $(N, 2N)$, but we skip a discussion of this).

By definition $Spec(R_N) = C(X^*)$ is the affine cone over the projective subvariety $j : X^* = A_{g,\kappa,N}^* \hookrightarrow \mathbb{P}$, since it is the ungraded ring of the corresponding graded coordinate ring of X^* . Therefore $Cl(R_N) = Cl(C(X^*))$ is obtained from $Cl(X^*)$ by

$$Cl(C(X^*)) = Cl(X^*)/\mathbb{Z} \cdot H$$

where H is the class corresponding to a hyperplane section H , which is a section of $j^*(\mathcal{O}_{\mathbb{P}}(1)) = \omega$. The cone $C(X^*)$ is normal and regular outside the isolated cusp and the singular lines over $X_s^* = X^* \setminus X_{reg}^*$. Since $g \geq 3$, the locus X_s^* has codimension ≥ 2 . Hence there exist canonical G_N -equivariant isomorphisms $Cl(C(X^*)) \cong Pic(C(X^*))$ and $Cl(X^*) = Pic(X^*)$ and $Cl(X) \cong Pic(X)$. The complement of $X_s = X \setminus X_{reg}$ in X_s^* also has codimension 2. Hence also $Cl(X) \cong Cl(X^*)$, and therefore $Pic(X^*) = Pic(X)$. The class of H therefore corresponds to the class of ω in $Pic(X)$. Hilbert theorem 90 implies

$$Cl(R_1) \hookrightarrow Cl(R_N)^{G_N}.$$

The composed map $\delta : Cl(R_N)^{G_N} \rightarrow H^1(G_N, Quot(R_N)^*/\kappa^*) \rightarrow H^2(G_N, \kappa^*)$ is trivial on the image of $Cl(R_1)$. A class x in $Cl(R_1)$ defines a class y in $Cl(R_N)$ with vanishing obstruction in $H^2(G_N, \kappa^*)$ (notice for $2|N$ this group may be nontrivial). Via the isomorphisms above there exists a corresponding class y^* in $Pic(X)/\mathbb{Z} \cdot c_1(\omega) \cong Pic(X^*)/\mathbb{Z} \cdot c_1(\omega) \cong Cl(X^*)/\mathbb{Z} \cdot j^*(\mathcal{O}(1)) \cong Cl(C(X^*))$, whose obstruction in $H^2(G_N, \kappa^*)$ vanishes in the sense of step 1 of the proof of the theorem. Hence by descend any representative $y \in Pic(A_{g,\kappa,N})$ of y^* is the pullback of a class from $Pic(A_{g,\kappa})$. However $Pic(A_{g,\kappa}) = \mathbb{Z} \cdot c_1(\omega)$ as shown in

the theorem for $p > p_0$. Therefore $y^* = 0$, hence $y = 0$ and $x = 0$. This proves $Cl(R_1) = 0$ for $p > p_0$, hence the unique factorization theorem. \square

References

- [C] Chai C.L., Compactification of Siegel moduli schemes, London Math. Soc. Lecture Notes Series 107, Cambridge university press, (1985)
- [CF] Chai C.L.-Faltings G., Degeneration of Abelian Varieties, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, vol. 22, Springer Verlag (1990)
- [D] Demazure M., Lectures on p -Divisible Groups, SLN 302, Springer Verlag (1972)
- [I] Igusa J.I., On the ring of modular forms of degree two over \mathbb{Z} , *Jorn. of Math.* 101, 1-3 (1979), 149 - 183
- [FD] Fiederowisz Z.-Priddy S., Homology of Classical Groups over a Finite Field, in *Algebraic K-theory* (Evanston 1976), edited by M.R.Stein, SLN 551, Springer Verlag, p. 269 - 282
- [F] Freitag E., Die Irreduzibilität der Schottkyrelation (Bemerkung zu einem Satz von J.Igusa), *Archiv Math.* vol. 40 (1983), 255 - 259
- [K] Katz N.M. p -adic properties of modular schemes and modular forms, *Modular Functions of One Variable III*, SLN vol. 350, Springer Verlag
- [K2] Katz N.M. A result of modular forms in characteristic p , *Modular Functions of One Variable V*, SLN vol. 601, Springer Verlag
- [MB] Moret-Bailly, L., Pinceaux de varietes abeliennes, *Asterisque* 129, (1985)
- [M] Mumford D., On the equations defining abelian varieties I, *Invent. Math.* 1 (1966), 287 - 354; 129 (1985)
- [M2] Mumford D., On the equations defining abelian varieties II, *Invent. Math.* 3 (1967), 75 - 135
- [S] J.P.Serre, Congruences et formes modulaires, *Seminaire Bourbaki* 1971/72, exp. 416, SLN 317
- [Sw] Swinnerton-Dyer H.P.F., On l -adic representations and congruences for coefficients of modular forms, *Modular functions in one Variable III*, SLN vol. 350, Springer Verlag